

IN THE CLAIMS:

Please amend the claims as indicated. A complete set of the claims is included below, reflecting added subject matter (*underlining*) and deleted subject matter (*strikethrough*), as well as the current status of each claim. This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for controlling access to a computer network, comprising:
 - gaining access to said computer network by use of a portable computing device;
 - reading biometric data peculiar to a user by the use of a biometric data reader coupled to said portable computing device;
 - if no previously stored biometric data is stored in said portable computing device,
 - determining if user of said portable computing device is authorized for network
 - use;
 - acquiring new biometric data if the user is authorized for network use;
 - storing said new biometric data;
 - comparing said biometric data peculiar to said user to previously stored biometric data stored in said portable computing device and said computer network for the purpose of identifying the user, and wherein said previously stored biometric data is operable to be removed from said portable computing device on instruction by a remote station on said computer network, said remote station retaining a copy of said biometric data; and
 - denying further access to said computer network and said portable computing device if said comparing step fails to identify said user as an authorized user.
2. (Original) A method as in Claim 1 wherein said access to said computer network is by use of a wireless connection.
3. (Original) A method as in Claim 1 wherein said biometric data is a fingerprint.

4. (Original) A method as in Claim 1 wherein said biometric data is an iris scan.
5. (Original) A method as in Claim 1 wherein said biometric data comprises one or more measured electrical characteristics.
6. (Original) A method as in Claim 1 wherein said biometric data can be programmed into said portable computing device by a remote station on said computer network.
7. (Canceled)
8. (Currently Amended) A method for controlling access to a portable computing device, comprising:
 - reading biometric data peculiar to a user;
 - if no previously stored biometric data is stored in said portable computing device,
 - determining if user of said portable computing device is authorized for network
 - use;
 - acquiring new biometric data if the user is authorized for network use;
 - storing said new biometric data;
 - comparing said biometric data with previously stored biometric data for the purpose of identifying the user, and wherein said previously stored biometric data is operable to be removed from said portable computing device on instruction by a remote station on a computer network, said remote station retaining a copy of said previously stored biometric data; and
 - preventing access to said computer network and said portable computing device if the user is not identified as an authorized user and powering down said portable computing device.

Application No.: 09/727,984
Preliminary Amendment dated: October 15, 2007
Reply to the Final Office Action of: March 19, 2007

9. (Previously Presented) A method as in Claim 8 wherein said biometric data is a fingerprint.
10. (Previously Presented) A method as in Claim 8 wherein said biometric data is an iris scan.
11. (Previously Presented) A method as in Claim 8 wherein said biometric data comprises one or more measured electrical characteristics.
12. (Previously Presented) A method as in Claim 8 wherein said previously stored biometric data stored in said portable computing device can be controlled by a remote station on said computer network.
13. (Currently Amended) An apparatus for controlling access to a computer network, comprising:
- a computer network, said computer network comprising one or more computer workstations, wherein access to said computer network is provided by said one or more workstations upon authentication of biometric data from a user;
 - a portable computing device, said portable computing device providing wireless access to said computer network and wherein said portable computing device is powered down upon unsuccessful authentication of biometric data from said user;
 - a biometric data reading device coupled to said portable computing device;
 - a data storage device for storing biometric data capable of identifying one and only one user; and
 - a wireless communication device coupled to said computer network, capable of enabling the loading and removing of said biometric data stored in said portable computing device, and wherein said biometric data is operable to be removed from said portable computing device on instruction by one of said one or more workstations on said computer network, said one of said one or more workstations retaining a

copy of said biometric data, said wireless communication device configured to determine if user of said portable computing device is authorized for network use and acquiring and storing new biometric data if the user is authorized for network use.

14. (Previously Presented) An apparatus as in Claim 13 wherein said portable computing apparatus comprises;
- a bus;
 - a memory unit coupled to said bus;
 - a data storage device coupled to said bus, capable of storing said biometric data;
 - a biometric data reader coupled to said bus;
 - a communication device coupled to said bus for communicating with a computer network; and
 - a processor coupled to said bus, said processor for performing a method for identifying a user by use of said biometric data, said method comprising the steps of :
 - reading applicable biometric data; and
 - comparing said biometric data with said biometric data stored in said memory unit.
15. (Previously Presented) An apparatus as in Claim 14 wherein said portable computing apparatus is a personal data assistant (PDA).
16. (Previously Presented) An apparatus as in Claim 14 wherein said biometric data reader is implemented as part of the portable computing apparatus.
17. (Previously Presented) An apparatus as in Claim 13 wherein said biometric data is a fingerprint.

Application No.: 09/727,984
Preliminary Amendment dated: October 15, 2007
Reply to the Final Office Action of: March 19, 2007

18. (Previously Presented) An apparatus as in Claim 13 wherein said biometric data is an iris scan.
19. (Previously Presented) An apparatus as in Claim 13 wherein said biometric data is any electronically storable identifying biometric data.
20. (Previously Presented) An apparatus as in Claim 13 wherein said biometric data comprises one or more measured electrical characteristics.
21. (Previously Presented) An apparatus as in Claim 13 wherein said computer network further comprises a remote station connected to said computer network.
22. (Previously Presented) An apparatus as in Claim 21 wherein said remote station is for performing a method of network access control, said method comprising:
uploading said biometric data from said portable computing apparatus;
downloading said biometric data to said portable computing apparatus; and
erasing said biometric data from said portable computing apparatus.